WHAT IS CLAIMED IS:

1. A method of managing a data object so as to comply with control conditions for usage of the data object, comprising:

storing a data object in the memory of a data object provider processor;

providing a variable number of control conditions for usage of the data object;

providing a general set of control data for the data object based on the variable number of control conditions for usage, the general set of control data comprising at least one or more usage control elements defining usages of the data object which comply with the variable number of control conditions; and

encrypting at least the data object to create a secure data package so that it is ready to transfer to a user data processor.

2. The method of Claim 1, additionally comprising encrypting together the data object and the general set of control data.

3. The method of Claim 1, wherein providing the general set of control data includes providing an identifier which uniquely identifies the general set of control data.

4. The method of Claim 1, wherein providing the general set of control data includes providing a security control element which identifies a security process to be applied before usage of the data object is allowed.

5. The method of Claim 1, wherein providing the general set of control data includes providing a format control element which identifies the format of the control data.

6. The method of Claim 1, additionally comprising:

receiving a request for authorization for usage by a user;

comparing the usage for which authorization is requested with the one or more usage control elements of the general set of control data; and

granting the authorization if the usage for which authorization is requested complies with the usages defined by the one or more usage control elements.

7. The method of Claim 6, additionally comprising requiring payment for the requested authorization for usage before granting the authorization.

8. The method of Claim 1, additionally comprising:

transmitting the secure data package into the data processor;

checking, in response to a request by a user for usage of the data object, whether the requested usage complies with the usage defined by the at least one usage control element of the general set of control data; and

decrypting, in response to the requested usage complying with the usage defined by the at least one usage control element of the general set of control data, the data object so as to enable the requested usage.

9. The method of Claim 8, additionally comprising:

combining, after the usage of the data object, the data object and the one or more usage control elements; and

reencrypting at least the data object.

10. A method of controlling the usage by a user of a data object so as to comply with control conditions for usage of the data object, comprising:

providing a variable number of control conditions for usage of the data object;

providing a data object and control data, which comprises at least one usage control element defining a usage of the data object which complies with the variable number of control conditions, the data object being encrypted;

receiving a request by the user for usage of the data object;

checking, in response to the request by the user for usage of the data object, whether the requested usage complies with the usage defined by the at least one usage control element of the control data; and

decrypting, in response to the requested usage complying with the usage defined by the at least one usage control element of the control data, the data object and enabling the requested usage.

11. The method of Claim 10, wherein the usage control element is updated after the at least one usage of the data object.

12. The method of Claim 10, wherein the control data comprises an indication of the number of times the user is authorized to use the data object in accordance with the at least one usage control element, wherein the requested usage of the data object is only enabled when the number of times is one or more, and wherein the number of times is decremented by one when the requested usage is enabled.

13. The method of Claim 10, wherein the control data comprise a security control element, and additionally comprising executing, before each usage of the data object, a security procedure defined in the security control element.

14. The method of Claim 10, wherein checking whether the requested usage complies with the usage defined by the at least one usage control element, comprises checking that a data processor is capable of executing a security procedure specified in a security control element of the at least one usage control element, and if not, disabling the usage.

15. The method of Claim 10, additionally comprising:

combining, after the usage of the data object, the data object and the one or more usage control elements; and

reencrypting at least the data object.

16. A system for managing a data object so as to comply with control conditions for usage of the data object, comprising:

a user interface module which receives a variable number of control conditions;

a packaging module which provides a general set of control data for the data object based on the variable number of control conditions for usage, the general set of control data comprising at least one or more usage control elements defining usages of the data object which comply with the variable number of control conditions and which packages the general set of control data; and

an encrypting module which encrypts the data object to create a secure data package, which is ready for transfer to a user.

17. The system of Claim 16, wherein the general set of control data comprises a control data element which controls further distribution of the data object.

18. The system of Claim 16, wherein one of the usage control elements includes a security control element that defines a security procedure.

19. A system for controlling the usage by a user of a data object so as to comply with control conditions for usage of the data object, comprising:

a usage manager module which receives a variable number of control conditions, checks whether a usage requested by the user complies with the usage defined by at least one usage control element that complies with the variable number of control conditions, and disables the usage requested by the user when the usage does not comply with the usage defined by the at least one usage control element; and

a decryption module which decrypts the data object, responsive to the check for requested usage by the usage manager module.

20. The system of Claim 19, wherein one of the usage control elements includes a security control element that defines a security procedure.

21. The system of Claim 20, wherein the security procedure is an RSA encryption algorithm.

22. The system of Claim 19, wherein the usage manager module encrypts the data object after usage.

23. A method of controlling the usage by a user of data objects so as to comply with a variable number of conditions for usage of the data objects, comprising:

providing at least two data packages, each data package comprising a data object and a user set of control data, which comprises at least one usage control element defining a usage of the data object which complies with the variable number of conditions, the data object being encrypted;

examining the usage control elements of the at least two data packages to find a match; and

performing an action being specified in the user sets of control data of the at least two data packages.

24. The method of Claim 23, wherein one of the at least two data packages is a sell order, and wherein one of the at least two data packages is a buy order.

25. The method of Claim 23, additionally comprising checking whether a data processor is capable of executing a security procedure specified in a security control element of the at least one usage control element, and disabling the usage when the data processor is not capable of executing the security procedure, and decrypting the data objects.

26. The method of Claim 25, additionally comprising:

updating the at least one usage control element of each data package; and reencrypting each of the data object.

27. A method of managing a data object so as to comply with a variable number of control conditions for usage of the data object, comprising:

providing variable control conditions for usage of the data object;

providing a general set of control data for the data object based on the variable control conditions for usage, the general set of control data comprising at least one or more usage control elements defining usages of the data object which comply with the variable control conditions;

providing, in response to a request for authorization for usage of the data object by a user, a user set of control data, which comprises at least a subset of the general set of control data, including at least one of the usage control elements;

encrypting at least the data object to create a secure data package; and

checking, before allowing transfer of the data package to the user, that the request for authorization for usage of the data object has been granted.

28. The method of Claim 27, additionally comprising checking whether a data processor is capable of executing a security procedure specified in a security control element of the at least one usage control element, and disabling the usage when the data processor is not capable of executing the security procedure.

29. The method of Claim 27, wherein the data object is composed of at least two constituent data objects and wherein the user set of control data, in response to a request for authorization for usage of one of the constituent data objects by a user, is created only for that constituent data object and combined only with a copy of that constituent data object.

30. The method of Claim 27, wherein the request for authorization is received from a user via a data network.

31. The method of Claim 27, wherein the data object is a composite d ata object including at least two constituent data objects, and wherein providing a general set of control data comprises providing a respective general set of control data for each of the constituent data objects and the composite data object, and wherein providing a user set of control data comprises providing a respective user set of control data for each of the constituent data objects and the composite data object.

32. The method as defined in Claim 27, additionally comprising storing the user set of control data in a processor of a data object provider.

33. The method as defined in Claim 27, additionally comprising:

transmitting the data package;

checking, in response to a request by the user for usage of the data object, whether the requested usage complies with the usage defined by the at least one usage control element of the user set of control data; and

decrypting, in response to the requested usage complying with the usage defined by the at least one usage control element of the user set of control data, the data object and enabling the requested usage.

34. The method of Claim 27, additionally comprising:

transmitting the data package; and

reencrypting the data object.

35. A system for managing a data object so as to comply with control conditions for usage of the data object, comprising:

a packaging module which provides a general set of control data for the data object based on variable conditions for usage, the general set of control data comprising at least one or more usage control elements defining usages of the data object which comply with the variable conditions and which combines the user set of control data with the data object, and wherein the packaging module provides in response to a request for authorization for usage of the data object by a user, a user set of control data, which comprises at least a subset of the general set of control data, which subset comprises at least one of the usage control elements;

an encrypting module which encrypts the data object to create a secure data package, which is ready for transfer to a user; and

a control module which checks that the request for authorization for usage of the data object has been granted before allowing transfer of the data package to the user.

36. A method of managing a data object so as to comply with control conditions for usage of the data object, comprising:

providing a general set of control data for the data object based on a variable number of control conditions for usage, the general set of control data comprising at least one or more usage control elements defining usages of the data object which comply with the variable number of control conditions; and

encrypting at least the data object to create at least one secure data package, which is ready for transfer to a user.

37. The method of Claim 36, wherein the data object and the usage control elements are encrypted into a single secure package.

38. The method of Claim 36, wherein providing the general set of control data includes providing a security control element which identifies a security process to be applied before usage of the data object is allowed.

39. The method of Claim 36, wherein providing the general set of control data includes providing a format control element which identifies the format of the control data.

40. The method of Claim 36, additionally comprising:

receiving a request for authorization for usage by a user;

comparing the usage for which authorization is requested with the one or more usage control elements of the general set of control data; and

granting the authorization if the usage for which authorization is requested complies with the usages defined by the one or more usage control elements.

41. A method of managing a data object at a data provider computer so as to comply with control conditions for usage of the data object, comprising:

providing a variable set of control data for the data object, the variable set of control data including usage information regarding the data object;

concatenating the variable set of control data with the data object; and

encrypting at least the data object to create at least one secure data package that is ready for transmission to a user data processor.

42. The method of Claim 41, wherein the encrypting includes storing the at least one secure data package at the data provider computer.

43. A method of managing a data object at a data provider computer so as to comply with control conditions for usage of the data object, comprising:

providing a set of control data for the data object based on a variable number of control conditions for usage, the set of control data including usage information regarding the data object;

combining the set of control data with the data object; and

encrypting at least the data object to create at least one secure data package, so that the at least one secure data package is stored in the data provider computer.

44. The method of Claim 43, additionally comprising transmitting the at least one secure data package to the user data processor.

45. The method of Claim 43, wherein the data object comprises digital money.

46. The method of Claim 43, wherein the data object comprises an empty file.

47. The method of Claim 43, wherein the data object is created by an author.

48. A method of managing a data object so as to comply with control conditions for usage of the data object, comprising:

storing a data object in the memory of a data object provider processor;

providing a variable number of control conditions for usage of the data object; and

providing a set of control data for the data object based on the variable number of control conditions for usage, the set of control data comprising at least one or more usage control elements defining usages of the data object which comply with the variable number of control conditions.

49. The method of Claim 48, additionally comprising:

transmitting the data object and the set of control data into a data processor; and

checking, in response to a request by a user for usage of the data object, whether the requested usage complies with the usage defined by the at least one usage control element of the set of control data; and

complying with the usage defined by the at least one usage control element of the set of control data so as to enable the requested usage.

50. The method of Claim 49, additionally comprising combining, after the usage of the data object, the data object and the one or more usage control elements.

51. The method of Claim 49, wherein the data object comprises digital data.

52. The data object of Claim 49, wherein the control data comprises an object identifier.

53. The data object of Claim 49, wherein the data object comprises a video file.

54. A security method comprising:

(a) digitally signing a first load module with a first digital signature designating the first load module for use by a first device class;

(b) digitally signing a second load module with a second digital signature different from the first digital signature, the second digital signature designating the second load module for use by a second device class having a tamper resistance and/or work factor substantially different from the tamper resistance and/or work factor of the first device class;

(c) distributing the first load module for use by at least one device in the first device class; and

(d) distributing the second load module for use by at least one device in the second device class.

55. An electronic appliance including:

a disk use arrangement for at least one of (a) reading information from, and (b) writing information to, a digital versatile disk optical storage medium; and

a secure node coupled to the disk use arrangement, the secure node providing at least one rights management process.

56. An electronic appliance including:

a disk use arrangement for at least one of (a) reading information from, and (b) writing information to, a digital versatile disk optical storage medium; and

at least one processing arrangement coupled to the disk use arrangement, the processing arrangement selecting at least some control information associated with information recorded on the storage medium based at least in part on the class of the appliance and/or the user of the appliance.

57. In an appliance capable of using digital versatile disks, a method including the following steps:

at least one of (a) reading information from, and (b) writing information to, a digital versatile disk optical storage medium; and

selecting at least some control information associated with information recorded on the storage medium based at least in part on the class of the appliance and/or the user of the appliance.

58. An electronic appliance including:

a disk use arrangement for reading information from a digital versatile disk optical storage medium; and

at least one processing arrangement coupled to the disk use arrangement, the processing arrangement protecting information read from the storage medium.

59. In an electronic appliance, a method including the following steps:

reading information from a digital versatile disk optical storage medium; and

protecting the information read from the optical storage medium.

60. An electronic appliance including:

a disk use arrangement for using information stored, or to be stored, on a digital versatile disk optical storage medium; and

at least one rights management arrangement coupled to the disk use arrangement, the rights management arrangement treating the storage medium and/or information obtained from the storage medium differently depending on the geographical and/or jurisdictional context of the appliance.

61. In an electronic appliance, a method including the steps of:

reading information from at least one digital versatile disk; and performing at least one rights management operation based at least in part on the geographical and/or jurisdictional context of the appliance.

62. An electronic appliance including:

a disk use arrangement for using at least one secure container stored on a digital versatile disk optical storage medium; and

at least one rights management arrangement coupled to the disk use arrangement, the rights management arrangement processing the secure container.

63. In an electronic appliance, a method including the following steps:

reading at least one secure container from at least one digital versatile disk; and

performing at least one rights management operation on the secure container.

64. An electronic appliance including:

at least one rights management arrangement for generating and/or modifying at least one secure container for storage onto a digital versatile disk optical storage medium.

65. In an electronic appliance, a method including the step of performing at least one rights management operation on at least one secure container for storage onto a digital versatile disk optical storage medium.

66. A digital versatile disk use system and/or method characterized in that the system and/or method uses at least one secure container.

67. An electronic appliance including:

a disk use arrangement for writing information onto and/or reading information from a digital versatile disk optical storage medium; and a secure arrangement that securely manages information on the storage medium such that at least a first portion of the information may be used on at least a first class of appliance while at least a second portion of the information may be used on at least a second class of appliance.

68. In an electronic appliance, a method including the following steps:

reading information from and/or writing information to at least one digital versatile disk optical storage medium;

using at least a first portion of the information on at least a first class of appliance; and

using at least a second portion of the information on at least a second class of appliance.

69. A system including first and second classes of electronic appliances each including a secure processing arrangement, the first appliance class secure arrangement securely managing and/or using at least a first portion of the information, the second appliance class secure arrangement securely managing and/or using at least a second portion of the information.

70. In a system including first and second classes of electronic appliances each including a secure arrangement, a method comprising:

(a) securely managing and/or using at least a first portion of the information with the first appliance class secure arrangement, and

(b) securely managing and/or using at least a second portion of the information with the second appliance class secure arrangement.

71. An electronic appliance including:

a disk use arrangement for writing information onto and/or reading information from a digital versatile disk optical storage medium; and a secure arrangement that securely stores and/or transmits information associated with at least one of payment, auditing, controlling and/or otherwise managing content recorded on the storage medium.

72. In an electronic appliance, a method including the following steps:

reading information from and/or writing information to at least one digital versatile disk optical storage medium; and

securely storing and/or transmitting information associated with at least one of payment, auditing, controlling and/or otherwise managing content recorded on the storage medium.

73. An electronic appliance including:

a disk use arrangement for writing information onto and/or reading information from a digital versatile disk optical storage medium;

a cryptographic engine coupled to the disk use arrangement, the engine using at least one cryptographic key; and

a secure arrangement that securely updates and/or replaces at least one cryptographic key used by the cryptographic engine to at least in part modify the scope of information usable by the appliance.

74. A method of operating an electronic appliance including:

writing information onto and/or reading information from a digital versatile disk optical storage medium;

using at least one cryptographic key in conjunction with said information; and

securely updating and/or replacing at least one cryptographic key used by the cryptographic engine key used by the cryptographic engine to at least in part modify the scope of information useable by the appliance.

75. A digital versatile disk appliance characterized in that at least one cryptographic key used by the appliance is securely updated and/or replaced to at least in part modify the scope of information that can be used by the appliance.

76. An electronic appliance having a class associated therewith, characterized in that at least one cryptographic key set used by the appliance class is selected to help ensure security of information released from at least one digital versatile disk.

77. In an electronic appliance including a disk use arrangement, a method comprising:

reading information from at least one digital versatile disk optical storage medium; and

persistently protecting at least some of the read information through at least one subsequent editing and/or production process.

78. In an electronic appliance, a method including the following steps:

reading information from and/or writing information to at least one digital versatile disk optical storage medium; and

securely managing information on the storage medium, including the step of using at least a first portion of the information on at least a first class of appliance, and using at least a second portion of the information on at least a second class of appliance.

79. A method of providing copy protection and/or use rights management of at least one digital property content and/or secure container to be stored and/or distributed on a digital versatile disk medium, comprising the step(s) of:

providing a set of use control(s) within a cryptographically encapsulated data structure having a predetermined format, the data structure format defining at least one secure software container for providing use rights information for digital property content to be stored on the digital versatile disk medium.

80. An arrangement for implementing a rights management system for controlling copy protection, use and/or distribution rights to multi-media digital property content stored or otherwise contained on a digital versatile disk, comprising:

an encrypted data structure defining a secure information container stored on an optical disk medium, the encrypted data structure including and/or referencing at least one content object and at least one control object associated with the content object, said content object comprising digital property content and said control object comprising rules defining use rights to the digital property content.

81. A rights management system for providing copy protection, use and/or distribution rights management for multimedia digital property content stored or otherwise contained on a digital versatile disk for access by an optical disk player device that uses digital property content stored on said optical disk medium, wherein said appliance includes a microprocessor controller for decrypting and using control rules and other selected encrypted information content encapsulated in the secure container by using a prescribed cryptographic key and applying said decrypted control rules to regulate use in accordance with control information contained within said control rules, so as to facilitate management of a diverse set of use and/or distribution rights which may be specific to different users and/or optical disk appliances, the system including:

an optical disk medium having stored thereon an encrypted data structure defining a secure information container, the encrypted data structure comprising and/or referencing at least one content object and at least one control object, said content object comprising digital property content, said control object comprising rules defining use rights associated with the digital property.

82. A method for providing copy protection, use and distribution rights management of multi-media digital property stored on and/or distributed via digital versatile disk, said optical disk medium having stored thereon an encrypted data structure defining a secure container for housing rights and/or copy protection

information pertaining to digital property content stored on the optical disk, wherein an optical disk player appliance for using digital property content stored on an optical disk must utilize a prescribed secure cryptographic key or set of keys to use the secure container, said data structure comprising one or more content objects comprising digital property content and one or more control objects comprising a set of rules defining use right to digital property, comprising the steps of:

(a) decrypting control rules and other selected encrypted information content encapsulated in the secure container using one or more cryptographic keys; and

(b) applying decrypted control rules to regulate use and/or distribution of digital property content stored on the optical disk in accordance with control information contained within the control rules, so as to provide customized use and/or distribution rights that are specific to different optical disk user platforms and/or optical disk appliances.

83. A rights management system for providing copy protection, use and/or distribution rights management of digital property stored or otherwise contained on a digital versatile disk, comprising:

a secure container means provided on an optical disk medium for cryptographically encapsulating digital property content stored on the optical disk, said container means comprising a content object means for containing digital property content and a control object means for containing control rules for regulating use and/or distribution of said digital property content stored on the optical disk.

84. In a system including plural electronic appliances at least temporarily connected to one another, a rights authority broker that determines what appliances are connected and specifies at least one rights management context depending on said determination.

85. An electronic appliance at least temporarily connected to a rights authority broker, the electronic appliance receiving at least one rights context from the rights authority broker when the device is connected to the rights authority broker.

86. A method of defining at least one rights management context comprising:

(a) determining whether a first electronic appliance is present; and

(b) defining at least one rights management control set based at least in part on the determining step (a).

87. A method of defining at least one rights management context including:

(a) coupling an optical disk storing information to an electronic appliance that can be selectively connected to a rights management broker;

(b) determining whether the electronic appliance is currently coupled to a rights management broker; and

(c) conditioning at least one aspect of use of at least some of the information stored on the optical disk based on whether the electronic appliance is coupled to the rights management broker.

88. An electronic appliance including:

an optical disk reading and/or writing arrangement;

a secure node coupled to the optical disk reading and/or writing arrangement, the secure node performing at least one rights management related function with respect to at least some information read by the optical disk reading and/or writing arrangement; and

at least one serial bus port coupled to the secure node, the serial bus port for providing any or all of the functions, structures, protocols and/or methods of IEEE 1394-1995.

89. A digital versatile disk appliance including:

means for watermarking content; and

serial bus means for communicating the watermarked content, wherein the serial bus means complies with IEEE 1394-1995.

90. An optical disk reading and/or writing device including:

at least one secure node capable of watermarking content and/or processing watermarked content; and

an IEEE 1394-1995 serial bus port.

91. An optical disk using system and/or method including at least some of the elements shown in FIG. 1.

92. An optical disk using system and/or method using at least some of the elements shown in FIG. 17.

93. An optical disk using system and/or method using at least some of the control set elements shown in FIG. 8a.

94. An optical disk using system and/or method using at least some of the elements shown in FIG. 15.

95. In a network including at least one electronic appliance that reads information from and/or writes information to at least one digital versatile disk optical storage medium, and securely communicates information associated with at least one of payment, auditing, usage, access, controlling and/or otherwise managing content recorded on the storage medium, a method of processing said communicated information including the step of generating at least one payment request and/or order based at least in part on the information.

96. A method of authenticating a load module comprising:

(a) authenticating a first digital signature associated with the load module, including the step of employing a first one-way hash algorithm, a first decryption algorithm, and a first public key; and

(b) authenticating a second digital signature associated with the load module, including the step of employing at least one of:

(i) a second one-way hash algorithm that is dissimilar to the first one-way hash algorithm,

(ii) a second decryption algorithm that is dissimilar to the first decryption algorithm, and

(iii) a second public key that is dissimilar to the first public key.

97. A protected processing environment comprising:

means for providing a tamper resistant enclosure;

means for maintaining at least one public verification key within the tamper resistant enclosure; and

means for authenticating load modules based, at least in part, on use of the public verification key.

98. A method of distinguishing between trusted and untrusted load modules comprising:

(a) receiving a load module,

(b) determining whether the load module has an associated digital signature,

(c) if the load module has an associated digital signature, authenticating the digital signature using at least one secret public key; and

(d) conditionally executing the load module based at least in part on the results of authenticating step (c).

99. A method of increasing the security of a virtual distribution environment comprising plural interoperable protected processing environments having different work factors, the method comprising:

(a) classifying the plural protected processing environments based on work factor,

(b) distributing different verification public keys to different protected processing environments having different work factor classifications, and

(c) using the distributed verification public keys to authenticate load modules, including the step of preventing protected processing environments having different work factor classifications from executing the same load module.

100. A protected processing environment, comprising:

a tamper resistant barrier having a first work factor; and

at least one arrangement within the tamper resistant barrier that prevents the protected processing environment from executing the same load module accessed by a further protected processing environment having a further tamper resistant barrier with a further work factor substantially different from the first work factor.

101. A method for protecting a computation environment surrounded by a tamper resistant barrier having a first work factor, the method including:

preventing the computation environment from using the same software module accessible by a further computation environment having a further tamper resistant barrier with a further work factor substantially different from the first work factor.

102. A method of protecting computation environments comprising:

(a) associating plural digital signatures with a load module;

(b) authenticating a first subset of the plural digital signatures with a first tamper resistant computation environment; and

(c) authenticating a second subset of the plural digital signatures with a second tamper resistant computation environment different from the first environment.

103. A computer security method comprising:

digitally signing, using a first digital signing technique, a first executable designating the first executable for use by a first device class; and

digitally signing, using a second digital signing technique different from the first digital signing technique, a second executable designating the second executable for use by a second device class having a tamper resistance and/or work factor substantially different from the tamper resistance and/or work factor of the first device class.

104. A method of authenticating an executable comprising:

(a) authenticating a first digital signature associated with the executable, including the step of employing a first one-way hash algorithm, a first decryption algorithm, and a first public key; and

(b) authenticating a second digital signature associated with the executable, including the step of employing at least one of:

(i) a second one-way hash algorithm that is dissimilar to the first one-way hash algorithm,

(ii) a second decryption algorithm that is dissimilar to the first decryption algorithm, and

(iii) a second public key that is dissimilar to the first public key.

105. A secure execution space comprising:

means for providing a tamper resistant barrier;

means for maintaining at least one public verification key within the tamper resistant barrier; and

means for authenticating executables based, at least in part, on use of the public verification key.

106. A method of distinguishing between trusted and untrusted executables comprising:

(a) receiving an executable;

(b) determining whether the executable has an associated digital signature;

(c) if the executable has an associated digital signature, authenticating the digital signature using at least one secret public key; and

(d) conditionally executing the executable based at least in part on the results of authenticating step (c).

107. A method of increasing the security of plural interoperable secure execution spaces having different work factors, the method comprising:

(a) classifying the plural secure execution spaces based on work factor;

(b) distributing different verification public keys to different secure execution spaces having different work factor classifications; and

(c) using the distributed verification public keys to authenticate executables, including the step of preventing secure execution spaces having different work factor classifications from executing the same executable.

108. A protected processing environment comprising:

a tamper resistant barrier having a first work factor; and

at least one arrangement within the tamper resistant barrier that prevents the secure execution space from executing the same executable accessed by a further secure execution space having a further tamper resistant barrier with a further work factor substantially different from the first work factor.

109. A method for protecting a computation environment surrounded by a tamper resistant barrier having a first work factor, the method including:

preventing the computation environment from using the same software module accessed by a further computation environment having a further tamper resistant barrier with a further work factor substantially different from the first work factor.

110. A method of protecting computation environments comprising:

(a) associating plural digital signatures with an executable;

(b) authenticating a first subset of the plural digital signatures with a first tamper resistant computation environment; and

(c) authenticating a second subset of the plural digital signatures with a second tamper resistant computation environment different from the first environment.

111. A rights management appliance including:

a user input device,

a user display device,

at least one processor, and

at least one element defining a protected processing environment,

characterized in that the protected processing environment stores and uses permissions, methods, keys, programs and/or other information to electronically manage rights.

112. In a rights management appliance including:

a user input device,

a user display device,

at least one processor, and

at least one element defining a protected processing environment,

a method of operating the appliance characterized by the step of storing and using permissions, methods, keys, programs and/or other information to electronically manage rights.

113. A rights management appliance including at least one processor element at least in part defining a protected processing environment, characterized in that the protected processing environment stores and uses permissions, methods, keys, programs and/or other information to electronically manage rights.

114. In a rights management appliance including at least one processor element at least in part defining a protected processing environment, a method comprising storing and using permissions, methods, keys, programs and/or other information to electronically manage rights.

115. An electronic appliance arrangement containing a protected processing environment and at least one secure database operatively connected to said protected processing environment, said arrangement including means to monitor usage of at least one aspect of an amount of appliance usage and control said usage based at least in part upon protected appliance usage control information processed at least in part through use of said protected processing environment.

116. In an electronic appliance arrangement containing a protected processing environment and at least one secure database operatively connected to said protected processing environment, a method characterized by the steps of monitoring usage of at least one aspect of appliance usage and controlling said usage based at least in part upon protected appliance usage control information processed at least in part through use of said protected processing environment.

117. A secure component-based operating process including:

(a) retrieving at least one component;

(b) retrieving a record that specifies a component assembly;

(c) checking said component and/or said record for validity;

(d) using said component to form said component assembly in accordance with said record; and

(e) performing a process based at least in part on said component assembly.

118. A secure component operating system process including:

receiving a component;

receiving directions specifying use of said component to form a component assembly;

authenticating said received component and/or said directions;

forming, using said component, said component assembly based at least in part on said received directions; and

using said component assembly to perform at least one operation.

119. A method comprising performing the following steps within a secure operating system environment:

providing code;

providing directions specifying assembly of said code into an executable program;

checking said received code and/or said assembly directions for validity; and

in response to occurrence of an event, assembling said code in accordance with said received assembly directions to form an assembly for execution.

120. A method for managing at least one resource with a secure operating environment, said method comprising:

securely receiving a first control from a first entity external to said operating environment;

securely receiving a second control from a second entity external to said operating environment, said second entity being different from said first entity;

securely processing, using at least one resource, a data item associated with said first and second controls; and

securely applying said first and second controls to manage said resource for use with said data item.

121. A method for securely managing at least one operation on a data item performed at least in part by an electronic arrangement, said method comprising:

(a) securely delivering a first procedure to said electronic arrangement;

(b) securely delivering, to said electronic arrangement, a second procedure separable or separate from said first procedure;

(c) performing at least one operation on said data item, including using said first and second procedures in combination to at least in part securely manage said operation; and

(d) securely conditioning at least one aspect of use of said data item based on said delivering steps (a) and (b) having occurred.

122. A method for securely managing at least one operation performed at least in part by a secure electronic appliance, comprising:

(a) selecting an item that is protected with respect to at least one operation;

(b) securely independently delivering plural separate procedures to said electronic appliance;

(c) using said plural separate procedures in combination to at least in part securely manage said operation with respect to said selected item; and

(d) conditioning successful completion of said operation on said delivering step (b) having occurred.

123. A method for processing based on independent deliverables comprising:

securely delivering a first piece of code defining a first part of a process;

separately, securely delivering a second piece of code defining a second part of said process;

ensuring the integrity of the first and second delivered pieces of code; and

performing said process based at least in part on said first and second delivered code pieces.

124. A method of securely controlling at least one protected operation with respect to a data item comprising:

(a) supplying at least a first control from a first party;

(b) supplying at least a second control from a second party different from said first party;

(c) securely combining said first and second controls to form a set of controls;

(d) securely associating said control set with said data item; and

(e) securely controlling at least one protected operation with respect to said data item based on said control set.

125. A secure method for combining data items into a composite data item comprising:

(a) securely providing a first data item having at least a first control associated therewith;

(b) securely providing a second data item having at least a second control associated therewith;

(c) forming a composite of said first and second data items;

(d) securely combining said first and second controls into a composite control set; and

(e) performing at least one operation on said composite of said first and second data items based at least in part on said composite control set.

126. A secure method for controlling a protected operation comprising:

(a) delivering at least a first control and a second control; and

(b) controlling at least one protected operation based at least in part on a combination of said first and second controls, including at least one of the following steps:

resolving at least one conflict between said first and second controls based on a predefined order;

providing an interaction with a user to form said combination; and

dynamically negotiating between said first and second controls.

127. A secure method comprising:

selecting protected data;

extracting said protected data from an object;

identifying at least one control to manage at least one aspect of use of said extracted data;

placing said extracted data into a further object; and

associating said at least one control with said further object.

128. A secure method of modifying a protected object comprising:

(a) providing a protected object; and

(b) embedding at least one additional element into said protected object without unprotecting said object.

129. A method for managing at least one resource with a secure operating environment, said method comprising:

securely receiving a first load module from a first entity external to said operating environment;

securely receiving a second load module from a second entity external to said operating environment, said second entity being different from said first entity;

securely processing, using at least one resource, a data item associated with said first and second load modules; and

securely applying said first and second load modules to manage said resource for use with said data item.

130. A method for negotiating electronic contracts, comprising:

receiving a first control set from a remote site;

providing a second control set;

performing, within a protected processing environment, an electronic negotiation between said first control set and said second control set, including providing interaction between said first and second control sets; and

producing a negotiated control set resulting from said interaction between said first and second control sets.

131. A system for supporting electronic commerce including:

means for creating a first secure control set at a first location;

means for creating a second secure control set at a second location;

means for securely communicating said first secure control set from said first location to said second location; and

means at said second location for securely integrating said first and second control sets to produce at least a third control set comprising plural elements together comprising an electronic value chain extended agreement.

132. A system for supporting electronic commerce including:

means for creating a first secure control set at a first location;

means for creating a second secure control set at a second location;

means for securely communicating said first secure control set from said first location to said second location; and

negotiation means at said second location for negotiating an electronic contract through secure execution of at least a portion of said first and second secure control sets.

133. A secure component-based operating system including:

component retrieving means for retrieving at least one component;

record retrieving means for retrieving a record that specifies a component assembly;

checking means, coupled to said component retrieving means and said record retrieving means, for checking said component and/or said record for validity;

using means, coupled to said checking means, for using said component to form said component assembly in accordance with said record; and

performing means, coupled to said using means, for performing a process based at least in part on said component assembly.

134. A secure component-based operating system including:

a database manager that retrieves, from a secure database, at least one component and at least one record that specifies a component assembly;

an authenticating manager that checks said component and/or said record for validity;

a channel manager that uses said component to form said component assembly in accordance with said record; and

an execution manager that performs a process based at least in part on said component assembly.

135. A secure component operating system including:

means for receiving a component;

means for receiving directions specifying use of said component to form a component assembly;

means, coupled to said receiving means, for authenticating said received component and/or said directions;

means, coupled to said authenticating means, for forming, using said component, said component assembly based at least in part on said received directions; and

means, coupled to said forming means, for using said component assembly to perform at least one operation.

136. A secure component operating environment including:

a storage device that stores a component and directions specifying use of said component to form a component assembly;

an authenticating manager that authenticates said component and/or said directions;

a channel manager that forms, using said component, said component assembly based at least in part on said directions; and

a channel that executes said component assembly to perform at least one operation.

137. A secure operating system environment comprising:

a storage device that stores code and directors specifying assembly of said code into an executable program;

a validating device that checks said received code and/or said assembly directors for validity; and

an event-driven channel that, in response to occurrence of an event, assembles said code in accordance with said assembly directions to form an assembly for execution.

138. A secure operating environment system for managing at least one resource comprising:

a communications arrangement that securely receives a first control from a first entity external to said operating environment, and securely receives a second control from a second entity external to said operating environment, said second entity being different from said first entity; and

a protected processing environment, coupled to said communications arrangement, that:

(a) securely processes, using at least one resource, a data item associated with said first and second controls, and

(b) securely applies said first and second controls to manage said resource for use of said data item.

139. A system for negotiating electronic contracts, comprising:

a storage arrangement that stores a first control set received from a remote site, and stores a second control set;

a protected processing environment, coupled to said storage arrangement, that:

(a) performs an electronic negotiation between said first control set and said second control set,

(b) provides interaction between said first and second control sets, and

(c) produces a negotiated control set resulting from said interaction between said first and second control sets.

140. A method for supporting electronic commerce including:

creating a first secure control set at a first location;

creating a second secure control set at a second location;

securely communicating said first secure control set from said first location to said second location; and

electronically negotiating, at said second location, an electronic contract, including the step of securely executing at least a portion of said first and second secure control sets.

141. An electronic appliance comprising:

a processor; and

at least one memory device connected to said processor;

wherein said processor includes:

retrieving means for retrieving at least one component, and at least one record that specifies a component assembly, from said memory device,

checking means coupled to said retrieving means for checking said component and/or said record for validity, and

using means coupled to said retrieving means for using said component to form said component assembly in accordance with said record.

142. An electronic appliance comprising:

at least one processor;

at least one memory device connected to said processor; and

at least one input/output connection coupled to said processor,

wherein said processor at least in part executes a rights operating system to provide a secure operating environment within said electronic appliance.

143. A method for auditing the use of at least one resource with a secure operating environment, said method comprising:

securely receiving a first control from a first entity external to said operating environment;

securely receiving a second control from a second entity external to said operating environment, said second entity being different from said first entity;

using at least one resource;

securely sending to said first entity in accordance with said first control, first audit information concerning use of said resource; and

securely sending to said second entity in accordance with said second control, second audit information concerning use of said resource, said second audit information being at least in part different from said first audit information.

144. A method for auditing the use of at least one resource with a secure operating environment, said method comprising:

securely receiving first and second control alternatives from an entity external to said operating environment;

selecting one of said first and second control alternatives;

using at least one resource;

if said first control alternative is selected by said selecting step, securely sending to said entity in accordance with said first control alternative, first audit information concerning use of said resource; and if said second control alternative is selected by said selecting step, securely sending to said second entity in accordance with said second control alternative, second audit information concerning use of said resource, said second audit information being at least in part different from said first audit information.

145. A method for automated negotiation, including the following steps:

creating a first rule set at a first site, the first rule set designed to participate in an automatic negotiation with a second rule set;

transmitting the first rule set from the first site to a second site,

at the second site, performing an automated negotiating process including:

comparing information present in or specified by the first rule set to a first requirement specified by a second rule set present at the second site;

if the comparison results in a first outcome, carrying out a first action, the first action including:

creating a secure container consisting of protected content and having an associated third rule set, the third rule set being created as a result of an interaction between the first rule set and the second rule set;

transmitting the secure container from the second site to the first site; and

using a rule from the third rule set to govern an aspect of access to or use of the protected content; and

if the comparison results in a second outcome, carrying a second action, which is different in at least one respect from the first action.

146. A method for automated negotiation, including the following steps:

creating a first rule set at a first site;

creating a second rule set at a second site;

transmitting the first rule set from the first site to a third site;

transmitting the second rule set to the third site;

at the third site, performing the following steps:

comparing a requirement specified by the first rule set to a requirement specified by the second rule set and determining that the requirements are consistent;

based at least in part on the results of the comparison, creating a third rule set, the third rule set including at least one rule specified at least in part by the first rule set and the second rule set;

associating the third rule set with a secure container;

encapsulating protected content into the secure container; and

transmitting the secure container to the first site.

147. A method for automated negotiation including the following steps:

generating a first rule set including a first rule from a first party which owns or at least in part controls governed content and a second rule from a second party which constitutes or includes a clearinghouse;

incorporating the governed content into a secure container;

storing the first rule set at a first site;

transmitting a second rule set from a second site to the first site, the second rule set including a third rule from a third party;

comparing at least a portion of the first rule set to at least a portion of the second rule set; and

based on the results of the comparison, providing access to the secure container to the third party.

148. A method of automated negotiation including:

creating a first rule set representing a negotiating position of a first party;

incorporating the first rule set into a first secure container;

creating a second rule set representing a negotiating position of a second party;

incorporating the second rule set into a second secure container;

selecting a negotiation site associated with a third party;

transmitting the first and the second secure containers to the negotiation site;

at the negotiation site, comparing an attribute of the first rule set to an attribute of the second rule set to determine whether the attributes are compatible and, depending on the results of the comparison, determining that the negotiation has succeeded, determining that the negotiation has failed, or determining that an additional comparison is required;

if the negotiation has succeeded, transmitting a third secure container to the first party, the third secure container containing governed content;

if the negotiation has failed, informing both parties of the failure, and not transmitting the third secure container to the first party; and

if an additional comparison is required, performing that comparison, and repeating until the negotiation either succeeds or fails.

149. A method including:

creating a first secure container including a first governed item and having associated a first control;

creating a second secure container including a second governed item and having associated a second control;

transferring the first secure container from a first location to a second location;

transferring the second secure container from a third location to the second location;

at the second location, obtaining access to at least a portion of the first governed item, the access being governed at least in part by the first control;

at the second location, obtaining access to at least a portion of the second governed item, the access being governed at least in part by the second control;

at the second location, creating a third secure container including at least a portion of the first governed item and at least a portion of the second governed item and having associated at least one control, the creation being governed at least in part by the first control and the second control.

150. A method of using a resource including the following steps:

receiving the resource at a first computing environment;

receiving a first control or control set at the first secure computing environment;

receiving a second control or control set at the first secure computing environment;

evaluating an auditing-related aspect of the first control or control set and the second control or control set, including evaluating a privacy-related aspect of the first control or control set and the second control or control set;

choosing between the first control or control set and the second control or control set, the choice being based at least in part on the evaluation; and

reporting auditing-related information relating to the access to or use of the resource to a second computing environment.